



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/304,444	05/03/1999	GREGORY BURNS	MS1-301US	9671

22801 7590 12/02/2004

LEE & HAYES PLLC  
421 W RIVERSIDE AVENUE SUITE 500  
SPOKANE, WA 99201

EXAMINER
----------

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 12/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/304,444

Applicant(s)

BURNS ET AL.

Examiner

Paula W Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 26 July 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1 and 3-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 3-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. This office action is in response to amendment filed on 07/26/04. Original application contained Claims 1-19. Applicant amended Claim 1, 7, and 17 and Claim 2 was cancelled. The amendment filed on 4/07/04 have been entered and made of record. Therefore, presently pending claims are 1 and 3-19.

### ***Response to Arguments***

2. Applicant's arguments filed 4/07/04 have been fully considered but they are not persuasive because of following reasons.

*In reference to claims 18 and 19*, the applicant argued that Sigbørnsen discloses the use of public key/private key technology for the purpose for which it was designed, i.e. encryption. The examiner would like to bring that applicants attention to column 7 lines 30 – 50 where Sigbørnsen discusses authentication in the card. Rejection of claims 18 and 19 are therefore maintained.

### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 1 and 3-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Herzi et al (6,353,885 B1).

*In reference to claims 1 and 7*, Jones discloses a system for safely porting user data from one computer to another (column 1 lines 60-65), comprising: a memory device to store the user data (part 100 of Fig. 1 in combination with column 9 lines 22-37); and a smart card (part 250 of Fig. 1 in combination with column 4 lines 59-65). The smart card is associated with a user because the user must know that password stored in the smart card for the smart card to release the information stored in the removable memory (column 3 lines 40-43 in combination with column 4 lines 59-67 in combination with column 5 lines 54-67). The smart card alternately enables access to the user data on the memory device when both the memory device and smart card are interfaced with a common computer and disables access to the user data when one of the memory device or smart card is absent (column 4 lines 47-67). The data from the PCMCIA card is only made available to the host if the enable signal is transmitted from the smart card; therefore the smart card and the host have to be at the same host. Access is disabled when the signal is not received.

Although Jones discloses a memory device that is removable connected to the host computer (column 9 lines 22-37), such as the remote computer, Jones does not expressly disclose a system that stores a user profile that can be used to configure a computer.

Herzi discloses a portable user profile carrier that is kept in the smart card and used to configure the user's computer (column 4 lines 40-51).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user's profile in a portable memory device as described in Herzi in the system disclosed by Jones. One of ordinary skill in the art would have been motivated to do this

Art Unit: 2135

because user would be required to identify themselves and, therefore gain access permission or not.

*In reference to claims 3 and 8*, Jones disclose a password (passcode) stored on a smart card and access to user data in the memory device being enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card (column 5 lines 54-67). A password, as defined by the Webster's dictionary, is something that enables one to pass or gain admission. Therefore, the pass code is a type of password. The comparing of the password entered by the user with the password stored in the smart card is a form of authenticating the smart card.

*In reference to claims 4, 9, and 10*, the system wherein the memory device stores a public key and the smart card stores a corresponding private key and access to the user data in the memory device is enabled upon verification that the public key and the private key are associated.

Jones discloses the smart card I.C storing a private key from the corresponding public key for a remote computer. Access is enabled upon verification that the public key and the private key are associated (column 9 lines 22-37 in combination with column 9 lines 5-15).

Jones does not expressly disclose the PCMCIA card storing the public key.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the public key in the PCMCIA card. One of ordinary skill in the art would have been motivated to do this because the information in the PCMCIA card is being protected just as the information in the remote computer is protected.

*In reference to claim 5*, Jones discloses a system comprising of a smart card and a memory device (part 100 of Fig. 1 in combination with column 1 lines 15-45 in combination

Art Unit: 2135

with part 250 of Fig. 1 in combination with column 4 lines 59-65). Jones disclose a password (passcode) stored on a smart card and access to user data in the memory device being enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card (column 5 lines 54-67). The memory device and the smart card in the system disclosed by Jones are interface with a common computing unit (column 4 lines 47-67). The data from the PCMCIA card is only made available to the host if the enable signal is transmitted from the smart card; therefore the smart card and the host have to be at a common host. Jones discloses a password stored on a smart card (column 5 lines 54-67). In addition Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The information stored on the local device can be stored on the smart card and the information on the remote device can be stored on the memory device. The user data would then only be made accessible when the correct private key and public key pair are applied. (The smart card is an integral part of the memory device).

Herzi discloses a user profile that is used to configure a computer (column 4 lines 40-51).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user profile disclosed by Herzi in the memory system disclosed by Jones. One of ordinary skill in the art would have been motivated to do this because functions that were previously performed within the confines of a secure office space are now done in the field (Jones column 1 lines 15-32). The system disclosed by Herzi would provide a method of saving the user's configuration in a smart card so that the user may reproduce the preferences chosen earlier (page 2 paragraph 0012).

*In reference to claim 6*, the memory device of Jones interfaces with the Host using a standard PCMCIA interface (column 4 lines 1-10). The UART performs that tasks of the smart card reader (part 230 Fig. 1).

*In reference to claim 11*, Jones discloses a system as in the rejection for claim 1.

However, Jones does not disclose a memory device to store the user's profile.

Herzi discloses a user's profile being stored in memory wherein the profile is accessible to configure the computer (column 4 lines 40-51).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to save the user's profile described by Herzi in the memory device described by Jones.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission.

*In reference to claim 12*, Jones disclose a password (passcode) stored on a smart card and access to user data in the memory device being enabled upon authentication of a user-supplied passcode to the passcode stored on the smart card (column 5 lines 54-67). A password, as defined by the Webster's dictionary, is something that enables one to pass or gain admission. Therefore, the pass code is a type of password. The comparing of the password entered by the user with the password stored in the smart card is a form of authenticating the smart card.

*In reference to claim 13*, Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The information stored on the local device can be stored on the smart card and the information on the

Art Unit: 2135

remote device can be stored on the memory device. The user data would then only be made accessible when the correct private key and public key pair are applied.

*In reference to claim 14*, Jones discloses a system where the IC card (smart card) stores a passcode (column 5 lines 54-67). Jones teaches of a remote device with a public key and a local device connected to a smart card that contains the private key, column 9 lines 24-42. The information stored on the local device can be stored on the smart card and the information on the remote device can be stored on the memory device. The user data would then only be made accessible when the correct private key and public key pair are applied.

*In reference to claim 15*, Jones discloses a computer system as in the rejection of claim 1.

Jones does not disclose a system for storing a user's profile for configuring the computer.

Herzi discloses a system where the user's profile is stored in memory for access for configuring the computer (column 4 lines 40-51).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the user profile, for configuring the computer that was described by Herzi, in the smart card secured memory system, described by Jones.

One of ordinary skill in the art would have been motivated to do this because it is desirable that the user identify themselves before gaining access permission.

*In reference to claim 16*, Jones discloses the computer system as applied to claim 15. Jones further discloses a system where data can be securely transported from one computer to a second computer (column 14 lines 20-30).



**Claim 17** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jones in view of Gilbert et al (5,987,138).

*In reference to claim 17*, Jones discloses a system containing a smart card and a portable memory device (part 100 Fig. 1); interfacing the smart card and the portable memory device with a computer (Fig. 3).

Although Jones discloses the smart card containing the public and private keys and authenticating using a pass code and allowing access to the user information, Jones does not disclose storing user data and a public key on a portable memory device storing a private key on a smart card and verifying compatibility of the public key and the private key.

However Gilbert discloses an identification and signature process wherein a claimant has a secret key and a verifier has a public key (Fig. 1). The verifier sends the claimant random numbers that the claimant uses to calculate the answer used to verify the claimant (column 7 lines 15-60). Wherein the verifier uses the result transmitted by the claimant and the public key to verify the claimant (column 7 lines 60-67).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to store the secret key of Gilbert in the smart card of Jones and the public key of Gilbert in the portable memory of Jones and perform the verification steps of Gilbert. One of ordinary skill in the art would have been motivated to do this because the steps disclosed by Gilbert perform calculations that are simple enough for a smart card that does not have a cryptographic processor.

**Claims 18 and 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over Jones and Herzi in view of Sigbjørnsen et al US 6,266,416 B1.

Jones discloses a system that stores user data in a portable memory device (column 1 lines 60-65). The PCMCIA card interfaces with the computer (column 4 lines 1-5). The smart card interfaces with the computer using the UART (Fig. 1 part 230). Jones discloses the smart card I.C storing a private key from the corresponding public key for a remote computer. In order, to protect information stored in the PCMCIA card the public key should be stored in the PCMCIA card as it was stored in the remote computer. Jones discloses a password stored in the smart card (Fig. 3 part 420). The system permits use of the card-resident key following validation of the user-entered passcode with the passcode stored in the smart card (column 5 lines 54-67). The card resident key and the device resident key are authenticated (column 9 lines 5-20). Access is enabled upon verification that the public key and the private key are associated (column 9 lines 22-37 in combination with column 9 lines 5-15).

Sigbjørnsen teaches of a system where an asymmetric authentication key is transferred to the smart card and decrypted in the smart card to initiate an authentication process in the smart card, column 7 lines 44-49.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art would use the system to store the password and a key on the smart card, store a corresponding key on the memory device, and transmitting the stored key from the memory device to the smart card in order to carryout the authentication.

One of ordinary skill in the art would have been motivated to do this because storing the password and a key on the smart card and a corresponding key on the memory device would

increase the security by requiring the user to be in possession of the memory card (which has the required keys) and the password, Jones column 9 lines 55-60. Carrying out authentication on the smart card give the users complete portability, user authentication can be carried out across operating systems and multiple computers.

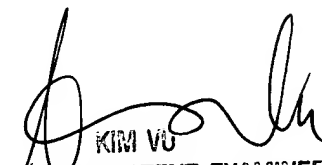
### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK  
Monday, November 29, 2004

  
KIM VU  
PRIMARY PATENT EXAMINER  
TECHNOLOGY CENTER 2100